
HACKER
LE HACKER
Apprenez à penser comme un hacker et à défendre votre chantier numérique comme un pro.
FORUMCONSTRUCTION 13/02
FEDERALE Verzekering
ALTIJD MEE, PRO EN PRIVÉ
fox & fish cyberdefense
beschermt terwijl u digitaliseert

LES HACKERS SONT PARESSEUX

(et c'est de notre faute)



fox & fish cyberdefense
beschermt terwijl u digitaliseert

Mathias Vissers

Hacker éthique et évangéliste
en cybersécurité
Fox&Fish

HACKER LE HACKER



Mon plaidoyer : Le pare-feu humain.

(contre les hackers paresseux)

HACKER LE HACKER

Schéma de la situation

Le cybercriminel

- Surtout pour l'argent
- Axé sur les organisations
- **Entreprises organisées**
- Confie le travail à des experts
- **Automatise autant que possible**
  - Obtenir autant de résultats que possible avec peu de travail manuel
  - Logiciels prêts à l'emploi pour l'hameçonnage, les « ransomwares », les réseaux de bots, ...




HACKER
LE HACKER





KK Park, één van de terreinen die cybercriminelen gebruiken als uitvalsbasis. © Google Earth / European Space Agency

Steenrijke cybercriminelen bouwen eigen 'stad' van waaruit ze de hele wereld oplichten: "Vroeger groene oase, nu plek met mensenhandel en foltering"

NET BINNEN

- 15:24 Nieuwe iPhone 17 kan volgens geruchten grootste update in jaren worden
- 10:00 Mobile Vikings lanceert mobiele abonnementen met aanpasbare snelheid
- 08:34 Musk beticht Apple van voortrekken ChatGPT en dreigt met rechtszaak
- 06:10 De helft van het budget voor je nieuwe smartphone slim bijeensparen?...
- 11-08 "Ik won dankzij dit woord een recordbedrag in spelprogramma op VTM"

MEER BERICHTEN

AD

STARLINK

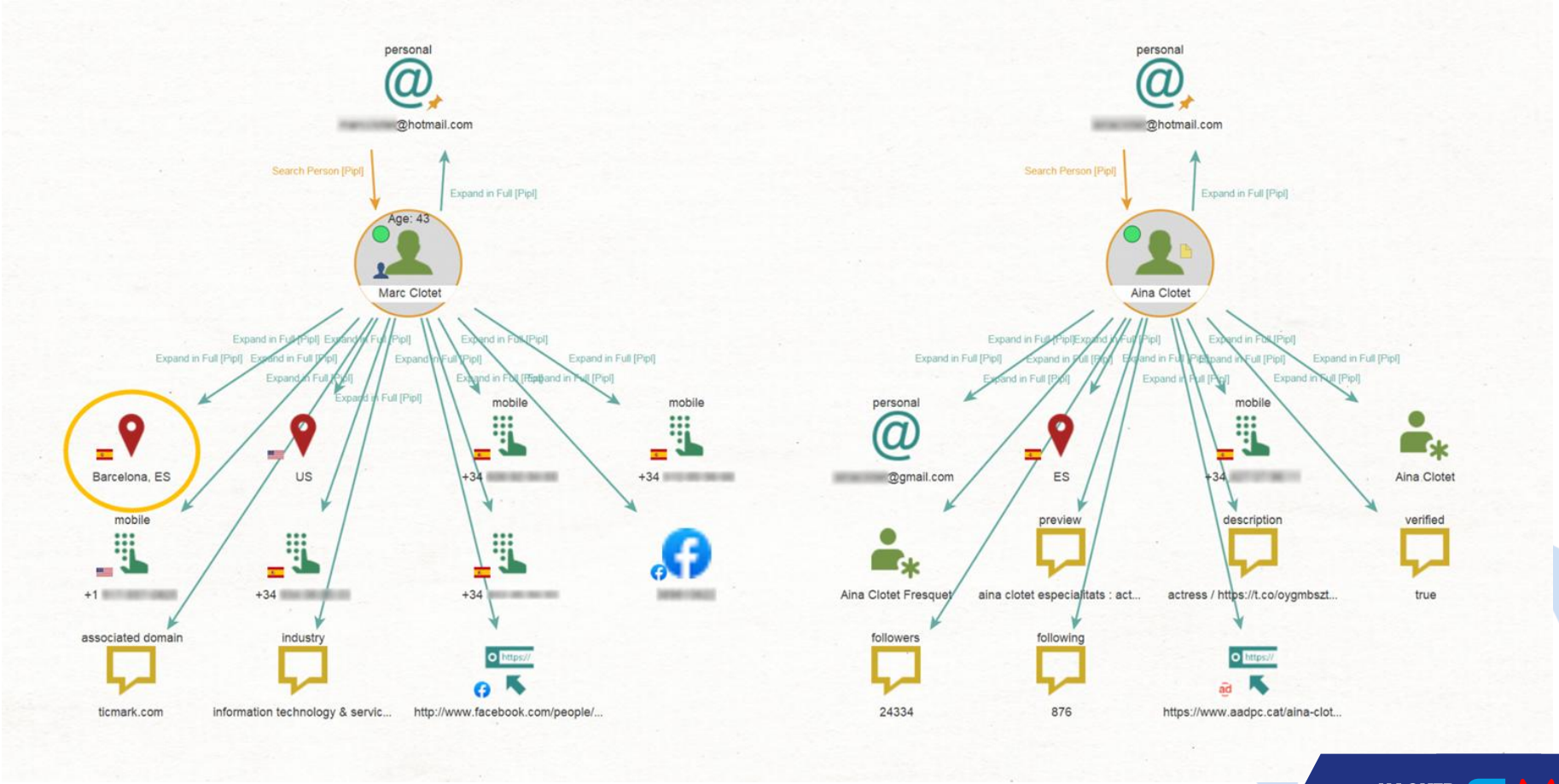
€ 99 ~~€ 299~~ voor de Standard-kit met een Residential-serviceabonnement met verbintenis van 12 maanden

HACKER LE HACKER

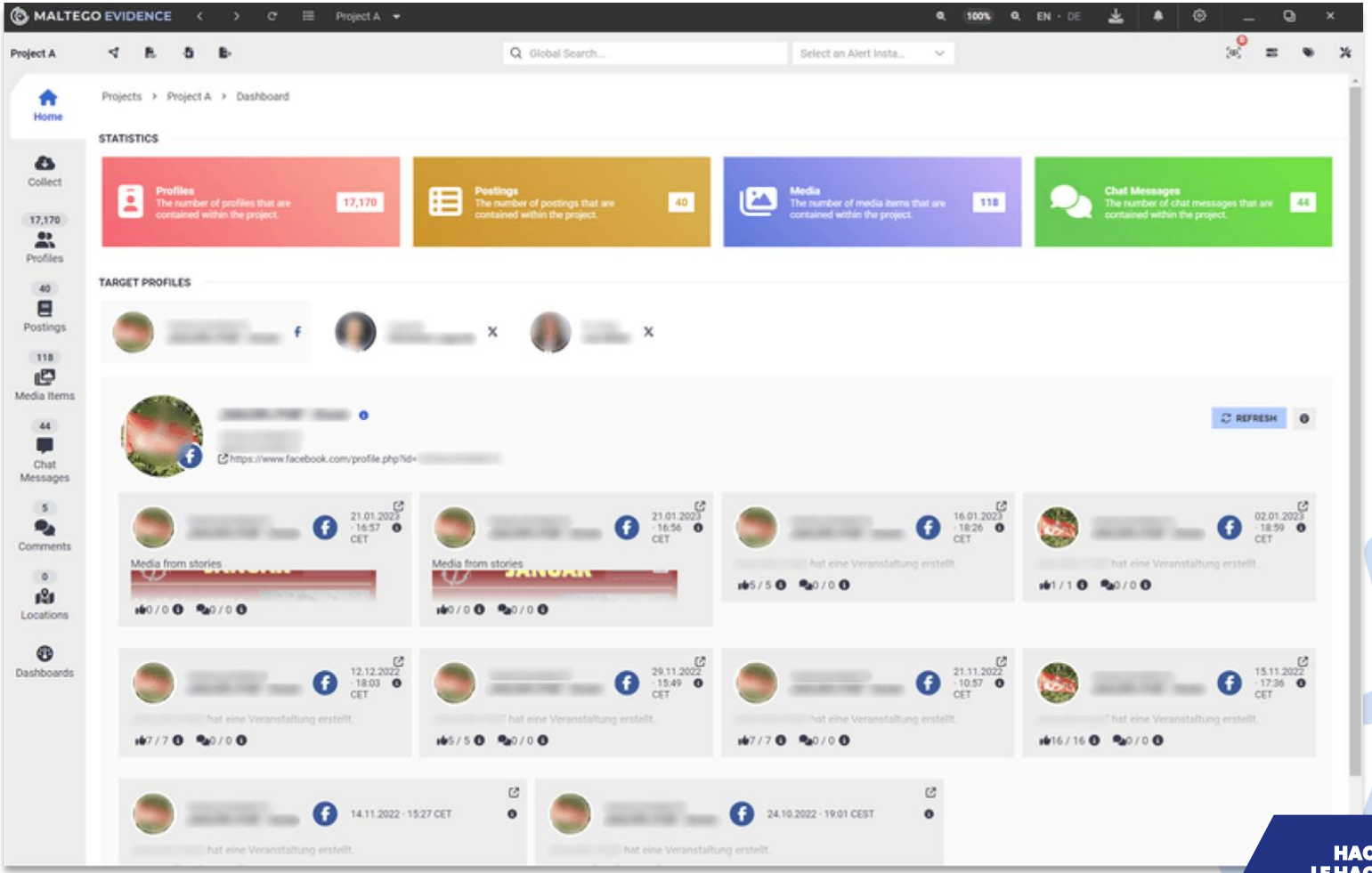
OSINT



Démonstration :
DataLeaks



HACKER LE HACKER



HACKER LE HACKER

Les fuites de données : la nouvelle norme

- ✓ Chaque semaine, une fuite de données fait la une de l'actualité.
- ✓ Une seule fuite de données n’est peut-être pas catastrophique.
- ✓ Les hackers combinent
  - Différentes fuites de données ;
  - Prennent les données depuis les réseaux sociaux ;
  - De manière automatisée.
- ✓ **Les différentes fuites de données permettent aux hackers de procéder à un phishing ciblé et convaincant.**

HACKER LE HACKER

Comment se protéger ?

- ✓ Réfléchissez à ce que vous publiez en ligne ;
  - Une fois en ligne, toujours en ligne
- ✓ Supprimez les profils et les comptes que vous n'utilisez plus ;
- ✓ Prenez le temps de configurer vos comptes de réseaux sociaux ;
- ✓ Soyez conscient des violations de données et de la manière dont ces informations peuvent être utilisées dans des escroqueries ;
- ✓ Sensibilisez vos collègues à la cybersécurité ;
- ✓ Si nécessaire, appliquer la politique ;

HACKER LE HACKER

Fuites de données et mots de passe

HACKER
LE HACKER

Trois options

1. Mots de passe faibles
2. Mots de passe réutilisés
3. Mots de passe reçus 🎁



Trois options

1. **Mots de passe faibles**
2. Mots de passe réutilisés
3. Mots de passe reçus 🎁



Un mot de passe sécurisé...

A. Comporte des lettres, des chiffres et des symboles

B. Ne contient aucune information vous concernant

C. Changements réguliers

D. Est composé d'au moins 12 caractères

Un mot de passe sécurisé...

A. Comporte des lettres, des chiffres et des symboles

B. Ne contient aucune information vous concernant

C. Changements réguliers

D. Est composé d'au moins 12 caractères



HACKER LE HACKER

Règles pour les mots de passe

- 123456
- azerty
- Louise
- Louise
- Louise1
- Louise_1
- Louise_2015
- Louise_2016

Pas de caractères consécutifs

Pas de mots de passe communs

Au moins 1 majuscule

Au moins 1 chiffre

Au moins 1 symbole

Au moins 10 caractères

Nouveau mot de passe obligatoire

HACKER LE HACKER

Démonstration : Conseils pour les mots de passe.

Les mots de passe complexes sont **difficiles** à retenir **pour les humains** et faciles à deviner par les ordinateurs.

Comment choisir un mot de passe à la fois sûr et convivial ?

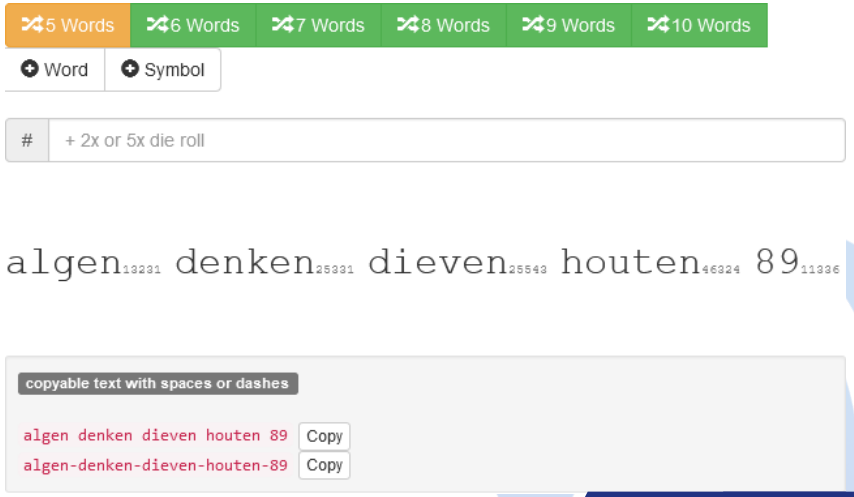
En ne le choisissant pas.

HACKER LE HACKER

https://password.utwente.io/nl/



https://www.rempe.us/diceware/#dutch



HACKER LE HACKER

Une phrase comme mot de passe

Roman fantasy

« Il est trop tard pour ouvrir la porte. » iettpolp

Livre sur le jardinage

« Il est préférable de planter une variété qui offre une résistance au champignon. » ilpdpuvqourac

Manuel du frigo

« Il se peut qu'il y ait un problème avec l'alimentation électrique de l'appareil. » ispqiyaupalaedla

HACKER LE HACKER

Trois options

1. Mots de passe faibles
2. **Mots de passe réutilisés**
3. Mots de passe reçus 🎁



À quel point votre mémoire est-elle bonne ?

- ★ L'internaute moyen a entre **100-200 identifiants**.
- ★ Combien de mots de passe (complexes) pouvez-vous retenir ?

Conséquence logique :

Nous réutilisons nos ~5 mots de passe préférés à l'infini.

HACKER LE HACKER

Démonstration : mots de passe sur le dark web.

Mais comment me souvenir de tout cela ?

Votre meilleur ami : le gestionnaire de mots de passe

- ✓ Génère des mots de passe uniques et sécurisés.
- ✓ Gestion simple et sécurisée de toutes vos données de connexion.
- ✓ Partager les données de connexion avec des collègues ou des membres de la famille.
- ✓ Connexion automatique à n'importe quel site web et appareil.
- ✓ Il vous suffit de générer et de mémoriser un **mot de passe principal**.

- ✓ **CONSEIL : notre préféré = 1Password.**

HACKER LE HACKER

3 règles pour les mots de passe

1. Ne les **choisissez** pas
2. Ne les **réutilsez** pas
3. Ne les **gardez** pas

HACKER LE HACKER

Notre conseil

- Rendez obligatoire l'utilisation d’un **gestionnaire de mots de passe** dans votre organisation.
- **Activez l'authentification multi-facteurs** (MFA) partout.
- Renforcez l'utilisation de mots de passe sécurisés via **une politique précise**.
- Sécurisez la **gestion** par des moyens supplémentaires comme des **tokens**.

HACKER LE HACKER

Trois options

1. Mots de passe faibles
2. Mots de passe réutilisés
3. **Mots de passe reçus** 🎁



Une perspective pour les mots de passe

Un hacker a **2 options** pour utiliser un mot de passe :

1. Essayer des identifiants sur des plate-formes
2. Cracker des mots de passe cryptés

Ces deux méthodes ont un taux de réussite relativement faible et prennent beaucoup de temps.

- Voler et cracker des mots de passe devient tranquillement **moins pertinent**.
- Plutôt applicable pour les **attaques ciblées.**

Les hackers préfèrent donc demander le mot de passe à leur cible

Phishing



Fuite de données = données personnelles + contexte



HACKER LE HACKER

GVA NIEUWS GEMEENTE SPORT CITTA BILLIE VIDEO ATV

Zelfs een telefoon van de CEO kan je niet vertrouwen: experts waarschuwen voor deepfake-phishing

Gilles Liesenborghs

Vrijdag 31 januari 2025 om 06:11



De cadeaubonnen van Apple, die Jana bestelde voor haar 'baas', kan je uitgeven in de winkel of via je iPhone en iPad. © ANP / EPA

Opgelicht tijdens haar stage: Jana (21) is geld kwijt, omdat ze naar 'baas' luistert

Met goede moed begint Jana* (21) aan haar stage bij de HR-afdeling van een bedrijf in Anderlecht. Wekenlang verloopt alles vlot tot ze een bericht krijgt in haar mailbox, waarin de grote baas vraagt of ze voor alle werknemers Apple-cadeaubonnen kan gaan kopen. Maar de mail blijkt afkomstig van criminelen te zijn.



Crelan 70 miljoen armer door één valse mail "van de baas"



© belga





70 miljoen euro, het is zowat de jaarwinst van bank en verzekeraar Crelan. Maar nu is die het bedrag in één klap kwijt. Omdat fraudeurs zich per e-mail voordeden als de grote baas, en het personeel op die manier de opdracht gaven om het geld naar hun rekening over te schrijven. Een bekende techniek, maar zelden met zo'n groot bedrag.

HACKER LE HACKER



NOS Nieuws • Zondag 2 mei 2021, 10:42

Bol.com maakt 750.000 euro over aan oplichters

Bol.com heeft in december 2019 en januari 2020 in totaal ruim 750.000 euro betaald aan oplichters. De webwinkel dacht het bedrag over te maken aan het bedrijf Brabantia, dat via Bol.com onder meer prullenbakken en andere huishoudelijke producten verkoopt. Maar het rekeningnummer bleek van oplichters. Bol.com moet het bedrag nu alsnog aan Brabantia betalen, oordeelt de rechter in een zaak die Brabantia had aangespannen.

Het ging mis toen Bol.com eind 2019 een e-mail ontving waarin stond dat het rekeningnummer van Brabantia was gewijzigd. De mail, opgesteld in gebrekkig Nederlands, was verstuurd vanuit het account van een medewerker van de boekhoudafdeling van het Brabantse bedrijf.

'Alle incoming betalingen have been overgemaakt'

"Houd he rekening mee dat we vanaf vandaag een wijziging in onze bankrekeninggegevens hebben voor incaende betalingen", staat in de mail. "Voortaan moten all incoming betalingen have been overgemaakt naar onze filiaalrekening in Spanje. We het op prijs as u uw gegevens kunt bijwerken."

brabantia

Tav: Account te betalen/Attn: Account Payable

Geachte heer mevrouw,

Houd he rekening mee dat we vanaf vandaag een wijziging in onze bankrekeninggegevens hebben voor incaende betalingen.

Voortaan moten all incoming betalingen have been overgemaakt naar onze filiaalrekening in Spanje.

We het op prijs as u uw gegevens kunt bijwerken.

Dear Sir / Madam,

Please be advised that we have a change in our bank account details for incoming payment with effect from today.

Henceforth all incoming payment should be transfer to our branch account in spain.

We would be obliged if you could update your records and direct all payment from today to new account below

ACCOUNT NAME: BRABANTIA International BV

BANK NAME: CAJAMAR CAJA RURAL, S.C.C

BANK ADDRESS: DE BARCELONA 5 4006 ALMERIA SPAIN

IBAN:

SWIFT BIC:

Should you have any queries please do not hesitate to contact us

Yours Sincerely,

Finance Director| Controlling

Chief Executive Off

HACKER LE HACKER

Phishing traditionnel

On peut le reconnaître avec les éléments suivants :

- Sentiment d'urgence
- Trop beau pour être vrai ou tente de provoquer la peur
- Le lien/bouton pointe vers un nom de domaine étrange
- L'e-mail de l'expéditeur est un nom de domaine bizarre
- Fautes ou structures de phrases étranges

Stratégie des hameçonneurs :

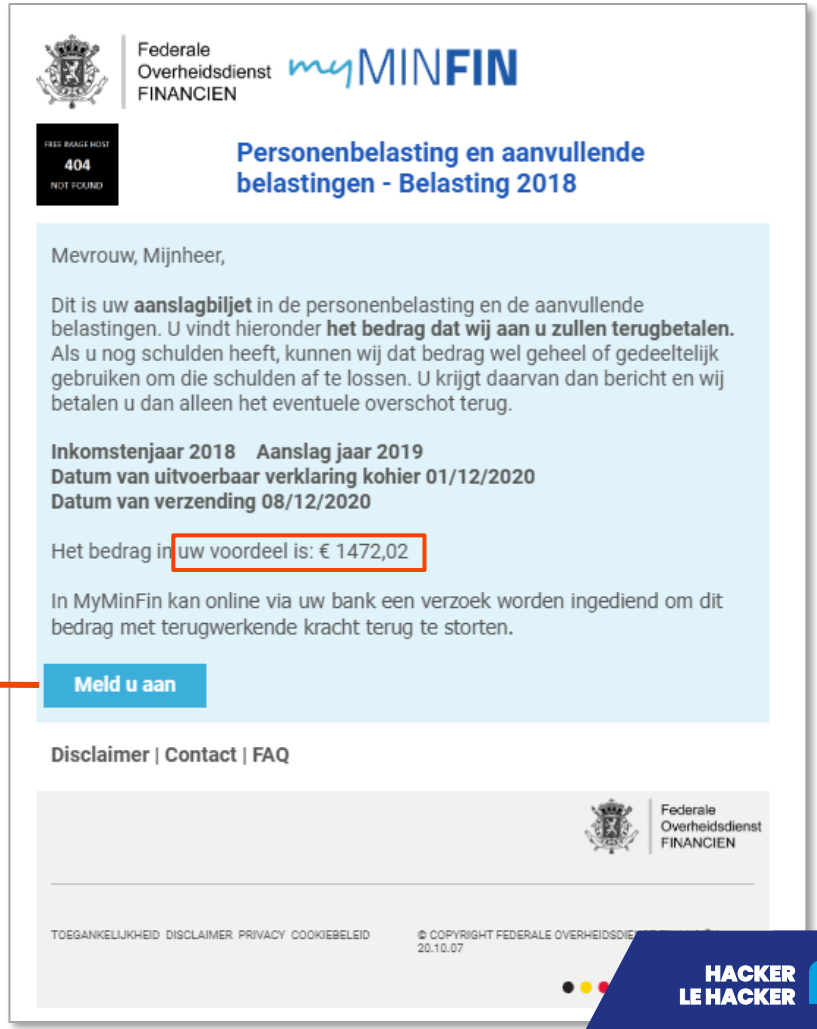
- Fréquence et volume
- Intelligence artificielle
- ...

HACKER LE HACKER

Phishing traditionnel

Van: "FOD MyMinFin" <support@mcpicky.com>
Aan: "michele [redacted]
Verzonden: Dinsdag 8 december 2020 13:07:00
Onderwerp: Terugbetaling personenbelasting en aanvullende belastingen 2018

https://kinkly.org/slCzUk6jE5/VV007wUw



Federale Overheidsdienst FINANCIEN myMINFIN

404 NOT FOUND

Personenbelasting en aanvullende belastingen - Belasting 2018

Mevrouw, Mijnheer,

Dit is uw **aanslagbiljet** in de personenbelasting en de aanvullende belastingen. U vindt hieronder **het bedrag dat wij aan u zullen terugbetalen.** Als u nog schulden heeft, kunnen wij dat bedrag wel geheel of gedeeltelijk gebruiken om die schulden af te lossen. U krijgt daarvan dan bericht en wij betalen u dan alleen het eventuele overschot terug.

Inkomstenjaar 2018 Aanslag jaar 2019
Datum van uitvoerbaar verklaring kohier 01/12/2020
Datum van verzending 08/12/2020

Het bedrag in uw voordeel is: € 1472,02

In MyMinFin kan online via uw bank een verzoek worden ingediend om dit bedrag met terugwerkende kracht terug te storten.

Meld u aan

Disclaimer | Contact | FAQ

Federale Overheidsdienst FINANCIEN

TOEGANKELIJKHEID DISCLAIMER PRIVACY COOKIEBELEID © COPYRIGHT FEDERALE OVERHEIDSDIE
20.10.07

HACKER LE HACKER

Phishing traditionnel

Beste Alvin Coessens,
Helaas moeten wij u meedelen dat vandaag de laatste kans is om uw cadeau te kiezen. Wij hebben u 4 weken geleden uitgekozen voor een kleine verrassing en ik heb al verschillende keren geprobeerd contact met u op te nemen.

Mijn collega Michael (vrachtafdeling) vertelde me dat er nog 2 andere mensen genomineerd zijn voor een cadeau. Als u niet reageert, krijgen zij het cadeau dat nog voor u gereserveerd is.

U kunt dit voorkomen door hier te bevestigen.

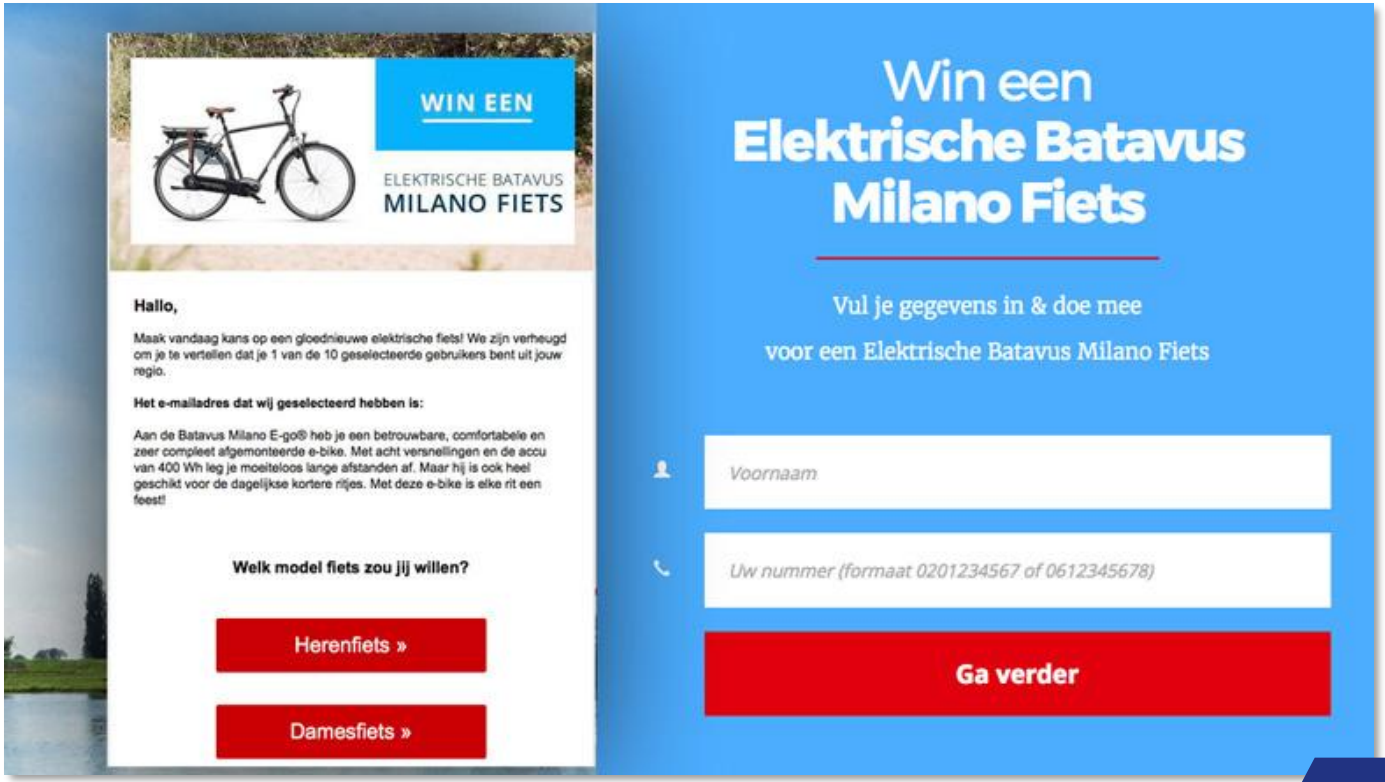
Genomineerde winnaars:

- Mohamed El hamdaoui
- Alvin Coessens
- Lisa steenkerken

Ontvang uw verrassing

HACKER
LE HACKER

« Créez un compte et gagnez »



HACKER
LE HACKER

Notre conseil

Le pare-feu humain

- **Formez vos collaborateurs** à reconnaître les e-mails de phising avec des **simulations de phishing.**
- Répétez sans cesse : **la sensibilisation pour un comportement cybersécuritaire**.
- Organisez des **formations obligatoires de sensibilisation à la cybersécurité.**
- Pour les paiements dépassant un certain montant, mettre en œuvre le principe de 2 ou 3 signataires comme paire d'yeux supplémentaire.

HACKER LE HACKER

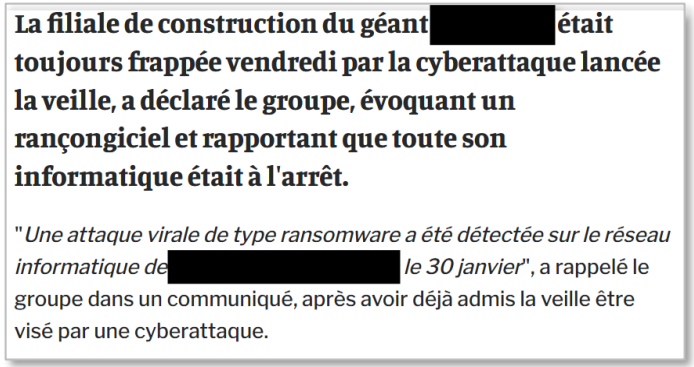

FEDERALE Verzekering
ALTIJD MEE, PRO EN PRIVÉ
LA CYBERSÉCURITÉ DANS LE SECTEUR DE LA CONSTRUCTION
HACKER LE HACKER


CELA VOUS SEMBLE FAMILIER ?
Les entreprises de construction ne sont pas été ciblées par les cybercriminels. Ce sont principalement les gouvernements,
Les petites entreprises ne sont pas visées.
NON-SENS
Mon entreprise est petite, il n'y a pas grand-chose à récupérer ici et pas grand-chose à perdre.
Un cyberincident ? Je dé
et cela résout mon problème.
HACKER LE HACKER



Ook Gents bouwbedrijf slachtoffer van cyberaanval met 'ransomware'

Na [redacted] is ook het Gentse bouwbedrijf [redacted], het slachtoffer geworden van een cyberaanval. Ook bij deze aanval maakten hackers gebruik van zogenaamde "ransomware": ze blokkeerden de computers en vroegen losgeld om het systeem opnieuw te activeren. Het bedrijf betaalde niet en zocht zelf een oplossing. Vanaf vandaag kunnen ze bij [redacted] weer aan de slag.



La filiale de construction du géant [redacted] était toujours frappée vendredi par la cyberattaque lancée la veille, a déclaré le groupe, évoquant un rançongiciel et rapportant que toute son informatique était à l'arrêt.

"*Une attaque virale de type ransomware a été détectée sur le réseau informatique de* [redacted] *le 30 janvier*", a rappelé le groupe dans un communiqué, après avoir déjà admis la veille être visé par une cyberattaque.

MYTHE

« Les entreprises de construction ne sont pas la cible des cybercriminels ».

FAIT

La construction est le 5e secteur touché.
dont les données sont sur le dark web (7 %).

Source : CS-Barometer

HACKER LE HACKER



Waarom cybercriminelen opnieuw meer kmo's en OT-systemen viseren

Mathias Caluwaerts

IT Solution Architect bij Orange Cyberdefense • 29-09-2025, 11:17 •



Cybersécurité en Belgique: les PME subissent 1.270 cyberattaques par semaine en 2025

MYTHE

« Les petites entreprises ne sont pas visées »

FAIT

60 % des entreprises touchées sont des PME.

HACKER LE HACKER



1 entreprise sur 2
(46 %) victimes d'une cyberattaque



Seulement 1 entreprise sur 5
dispose d'un plan de cybersécurité.



90 % des attaques
commencent par une erreur humaine (p.ex. le phishing).

Les chiffres ne mentent pas



1 entreprise sur 7
perd des revenus après une attaque



Prix moyen : **440 000 € par incident**

HACKER LE HACKER


FEDERALE
Verzekering
ALTIJD MEE, PRO EN PRIVÉ
ÉVALUEZ
VOTRE RISQUE
HACKER
LE HACKER

La « Cyber Roadmap »



1. LE DANGER

Comment les hackers opèrent-ils ?



2. QUELS SONT LES ENJEUX ?

Quelles sont les conséquences possibles pour votre entreprise ?



3. PRÉVENTION

Comment protéger votre entreprise contre ce phénomène ?



Transfert de risques



Acceptation des risques

4. ÉVALUATION DU RISQUE RÉSIDUEL

Quelles sont les chances ?
Quelles sont les conséquences ?
Est-ce que je veux prendre ce risque ?

HACKER LE HACKER

La « Cyber Roadmap »



1. LE DANGER

Comment les hackers opèrent-ils ?



2. QUELS SONT LES ENJEUX ?

Quelles sont les conséquences possibles pour votre entreprise ?



3. PRÉVENTION

Comment protéger votre entreprise contre ce phénomène ?





4. ÉVALUATION DU RISQUE RÉSIDUEL

Transfert de risques

Acceptation des risques

Quelles sont les chances ?
Quelles sont les conséquences ?
Est-ce que je veux prendre ce risque ?

Créer un plan d'intervention en cas d'incident

- ✓ Isoler l'incident
- ✓ Trouver des traces
- ✓ Restaurer
- ✓ Prévenir
- ✓ Déposer une plainte

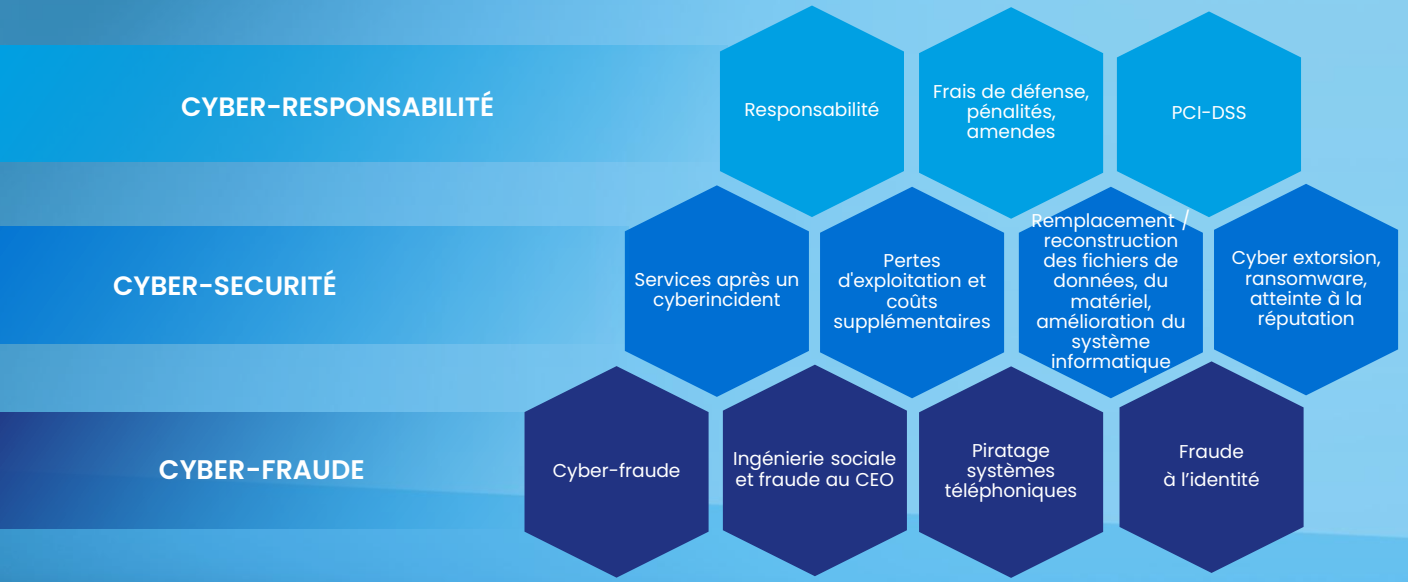
Cyberassurance

Gestion de crise incluse !

HACKER LE HACKER


LA CYBERASSURANCE
TOUT DANS LES MAINS
DES EXPERTS
HACKER
LE HACKER

Les éléments constitutifs de la cyberassurance
chez Fédérale Assurance



HACKER LE HACKER

Accent sur la prévention

Audits, sensibilisation et politique.

Mesures de prévention

= condition de la souscription

Ressources disponibles :

Pour les micro-entreprises :

Formation de sensibilisation gratuite pour les collaborateurs dans F-Cyber Comfort.

Pour les PME :

Le gouvernement flamand accorde jusqu'à 45% de subventions
pour votre cybersécurité grâce au **Portefeuille PME de VLAIO**.

VLAIO

HACKER
LE HACKER


« Le pare-feu humain empêche plus d'incidents que que votre pare-feu informatique. »
HACKER LE HACKER

Rendons le piratage économique moins intéressant.

...

(car les hackers sont paresseux)



🔐 Rien n'est inviolable

- Et ce n’est pas nécessaire
- Mais le seuil pour les criminels devient de plus en plus bas avec les logiciels disponibles sur le marché.

🔗 L'humain est le maillon faible

- Investir dans la sensibilisation et la formation.
- Pensez également au personnel de direction.

🏰 Il n'est pas nécessaire d'être Fort Knox

- Il suffit d'être une cible moins intéressante que son voisin.

🛡️ Décidez d'assurer ou d'accepter votre « risque résiduel ».

- Dans tous les cas, assurez-vous d'avoir un plan d'intervention en cas d'incident.

Une approche éprouvée pour vous protéger

Nous nous appuyons sur cinq piliers pour vous protéger contre les cyberattaques :

Audits et analyse des risques
de votre organisation

Formation et sensibilisation
de vos collaborateurs

Détection, mise en œuvre et sécurisartion
de votre infrastructure informatique

Stratégie et politique en matière de cybersécurité

Une cyber-assurance pour couvrir votre risque résiduel

HACKER LE HACKER

Merci pour votre attention !

Vous voulez en savoir plus sur la cyber-assurance ?

DEMANDEZ UN RENDEZ-VOUS !

go.federal.be/fr-event

Votre organisation sur le dark web ?

FAITES UN DARKWEB SCAN !

foxandfish.be/darkweb

HACKER LE HACKER